Detecting Distributed Denial-of-Service Flooding Attacks using Detection and Defense Algorithm

U. Leela Krishna[#1], Maddali M. V. M. Kumar[#2]
[#1]PG Student, Dept. of MCA, St. Ann's College of Engineering & Technology, Chirala.
[#2]Assistant Professor, Dept. of MCA, St. Ann's College of Engineering & Technology, Chirala.

Abstract— These days, computer arranges is critical in view of the many focal points it has. Be that as it may, it is likewise powerless against a great deal of dangers from aggressors and the most well-known of such attack is the Distributed Denial of Service (DDoS) attack. This paper introduces an outline of the current identification and barrier algorithms to alleviate four sorts of DDoS attacks and they are the UDP surge, TCP SYN surge, and Ping of Death and Smurf attack. A discovery and protection algorithm will be proposed in this paper and it will be assessed utilizing the current Intrusion Detection and Prevention apparatus to decide if it is the best algorithm to moderate the DDoS attacks on a system situation. The proposed algorithm will be estimated as far as false positive rates and location exactness.

Keywords—DDoS, detection and defense algorithm, TCP SYN flood, UDP flood, ping of death and Smurf attack.

1. Introduction

These days, system and information are powerless against organize attacks which may incorporate DDoS attacks propelled by assailants around the globe to upset the system condition. DDoS attacks are ordered as the most mainstream arrange attack on the grounds that the attacks are most regular around the globe. Also, DDoS attack is anything but difficult to execute on the grounds that its attack technique is basic yet hard to barrier. There are a few sorts of DDoS attacks, for example, UDP surge, TCP SYN surge, Ping of Death, Smurf attack, DNS enhancement attacks, HTTP surge and Slowloris .

2. Types of DDoS Attacks and Its Effects

The essential of a DDoS attack is appeared in Fig. 1, where an aggressor utilizes a few Zombies to make the attack more grounded on the casualties. There are three classes of DDoS attacks: volume-based attack, protocol attack and application layer attack. Volume-based attack will surge the data transfer capacity of the attacked site and it is estimated in bits every second. This sort of attack incorporates UDP surge, ICMP surge and other satirize packet surge. The protocol attack then again will hinder real server assets and it is estimated in packets every second. This incorporates TCP SYN surge, divided packet attack, Ping of Death and Smurf attack. The latter is the application layer attack where it will crash the web server and it is estimated in demands every second. This paper just concentrates on four sorts of DDoS attacks: UDP surge, TCP SYN surge, and Ping of Death and Smurf attack. These four sorts of

DDoS attacks are normal and extremely prominent system attack propelled by aggressors. Also, it is anything but difficult to execute in light of the fact that its attack technique is basic, yet hard to barrier. Despite the fact that much research has been completed to distinguish and barrier distinctive kinds of DDoS attacks all through the world, still new techniques for discovery and resistance errand should be explored in battling the endless attacks on the system as innovation changes quickly thus does the system attack.

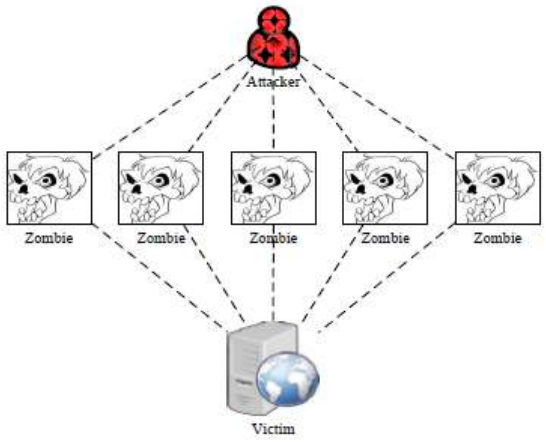

Fig. 1. Basic of DDoS attacks.

A. UDP Flood UDP is a connectionless protocol in which there is no association set up before information transmission between the sender and collector. Likewise, UDP can't recognize the packet misfortune amid the information transmission and it can't send any mistake message. The greatest favorable position of UDP contrasted with TCP is its high transmission speed. In any case, UDP packets can be misused by assailants to dispatch UDP surge attacks, for example, high transfer speed attacks. UDP surge is propelled by sending countless packets to irregular goal ports to the casualty's computer and this will back off the computer framework and accidents it as appeared in Fig.2.

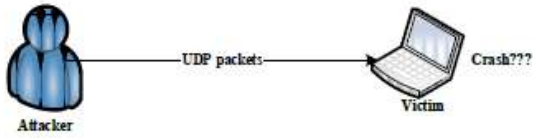

Fig. 2. UDP Flood attack.

B. TCP SYN Flood In the TCP connection, customer and server association ought to be built up first before information transmission. This is called TCP three-way handshake. The customer needs to send SYN message to the server, at that point the server will recognize this by sending SYN-ACK message to the customer and the customer needs to send ACK message to the server and the association is built up. Notwithstanding, the typical TCP three-way handshake will transform into a TCP SYN surge when the assailant sends rehashed SYN packets to arbitrary port on the focused on server by utilizing a phony IP address as appeared in Fig. 3. The server will confront a few issues, for example, trouble in shutting the (association remains open) and dependably get an extensive number of SYN packets but then no reaction is made to genuine the customers and this can crash the server.

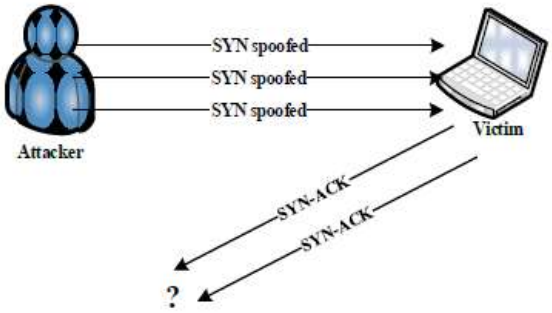

Fig. 3. TCP SYN Flood attack.

C. Ping of Death The most extreme size of the IP packet is 65535 bytes including the headers. The computer frameworks were never created to deal with a ping packet bigger than the most extreme packet measure since it can disregard the IP. Ordinarily, the assailants send contorted packets in parts. The section will be reassembled by the objective framework, yet the packet is curiously large and this will make the memory floods and prompt different framework issues, including crashes as appeared in Fig. 4. Ping of Death can be considered as a viable attack in light of the fact that the aggressor's detail can be effectively caricature. In addition, the aggressor will require no nitty gritty information of the casualty's computer aside from its IP deliver to dispatch the Ping of Death attack.

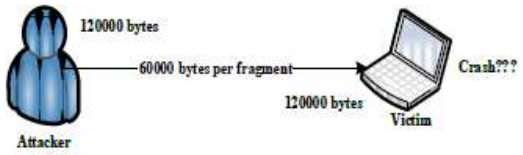

Fig. 4. Ping of Death Attack.

D. Smurf: Smurf attack is propelled by sending an extensive number of ICMP packets to the casualty's computer and the computer framework is overflowed with mock ping messages as appeared in Fig. 5. There are five stages engaged with propelling an effective Smurf attack. The effect of a fruitful Smurf attack among others are disabled organization server which may keep going for quite a long time or days, lost income, client dissatisfaction and robbery of records or other licensed innovation. Numerous Smurf attacks come packaged with rockets that enable assailants to make a secondary passage for simple framework access and it can bring down a server or site of an organization regardless of whether the aggressor dispatches the attack utilizing just small ping traffic.

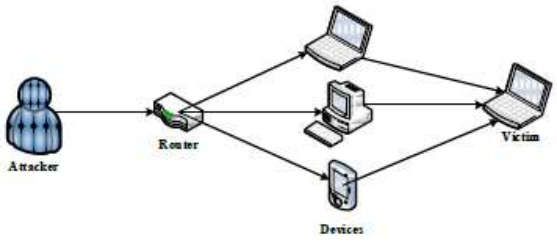

Fig. 5. Smurf attack.

E. Current Ddos Detection and Defense Algorithms DDoS attacks are exceptionally common and moderately simple to execute to intrude on a system situation. This is the motivation behind why associations need an approach to recognize and resistance against DDoS attacks. There are a few current algorithms intended to recognize and resistance diverse kinds of DDoS attacks. The design and execution of an Artificial Immune System in light of Dendritic Cell Algorithm. The framework was utilized to recognize DDoS attack and reaction to the location action to its generator. Nonetheless, the algorithm is utilized for TCP SYN surge attack discovery. The investigation led by then again concentrates on the plan of the ICMP trace back in light of the Packet Marking Algorithm to distinguish DDoS attack. There are two assessment strategies utilized. The main technique utilizes a virtual machine to execute the trackback framework. The second strategy utilizes a reenactment to assess the quantity of packets required to recognize the aggressors, who propelled the attack. The algorithm is utilized for Smurf attack recognition. The

investigation takes a gander at the trace back framework by applying Packet Marking Algorithm to distinguish and avoid DDoS attack and recognize the assailant's host data, regardless of whether they utilize mock IP address. The specialists test and assess the trackback framework as far as number of packets, time of preparing for remaking and number of attack sources. Like the past examination, this algorithm is utilized for TCP SYN surge attack location. Then an examination concentrates on Packet Marking Algorithm to channel DDoS attack that contained unique finger impression to recognize attack packets originating from different sources even in the event of IP satirizing. The scientists utilize the OMNET++ test system to decide the algorithm can recognize the aggressor way stamp and can alleviate the dangers of TCP SYN surge attack. This algorithm is utilized for TCP SYN surge attack identification. The algorithms composed hitherto are gone for just identifying and defending against TCP SYN surge, while there different kinds of attacks, for example, Ping of Death, Smurf attack, DNS enhancement attack, HTTP surge and Slowloris that should be recognized.

3. Research Methodology Framework

There are seven phases in conducting this research as outlined in Fig. 6.

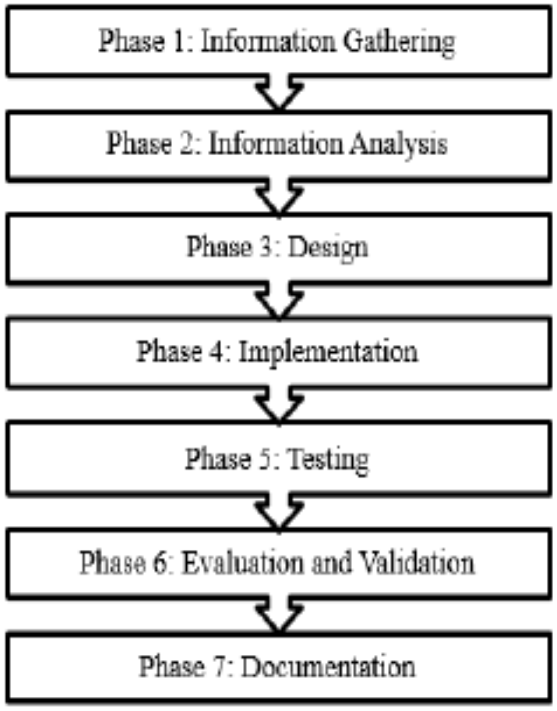

Fig. 6. Research methodology framework.

The primary stage is Information Gathering, where it is utilized to discover writing identified with the meaning of DDoS attacks, kinds of DDoS attacks, how the DDoS attacks work and to consider the conduct of DDoS attacks when the system is under attack. The second stage is Information Analysis, where it is utilized to discover a few current DDoS identification and aversion algorithms, at that point think about them and select the suitable algorithms in light of some choice criteria. The third stage is Design, where it is utilized to outline DDoS location and defense algorithms to identify and resistance against UDP surge, TCP SYN surge, and Ping of Death and Smurf attacks and propose a report of attacks to log particular data about the DDoS attack distinguished. The fourth stage is Implementation, where it is utilized to actualize the proposed algorithms by executing the proposed algorithms to recognize and make a shield framework against UDP

surge, TCP SYN surge, and Ping of Death and Smurf attack. The fifth stage is testing, where it used to test the proposed algorithms to quantify the proposed algorithms regarding false positive rates and discovery exactness. The 6th stage is Evaluation and Validation, where the trial result is displayed in a specific outline. The seventh stage is Documentation, where the examination will be reported in a specific postulation design.

4. Proposed Algorithms

This examination will concentrate on planning another DDoS recognition and resistance algorithms to relieve UDP surge, TCP SYN surge, Ping of Death and Smurf attack. In the proposed algorithm, it concentrates on three vital parts: location, defense and report of attacks as appeared in Fig. 7.

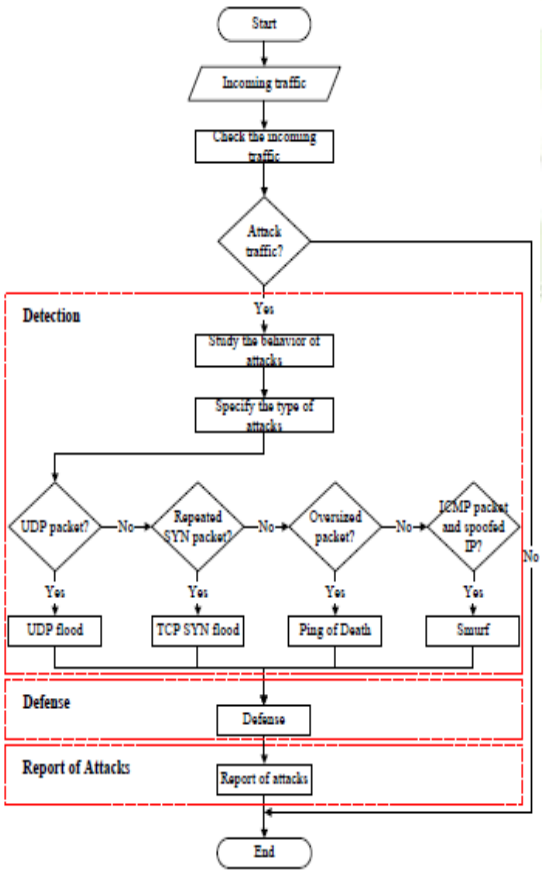

Fig. 7. Proposed design.

A. Detection DDoS detection is exceptionally fundamental to the system condition to recognize DDoS attacks in light of the fact that the attack is greatly simple to execute. The proposed recognition algorithm is appeared in Fig. 8. The proposed recognition algorithm will check the approaching activity, regardless of whether it is DDoS movement or ordinary movement. On the off chance that the approaching movement is DDoS activity, the proposed identification algorithm will determine the sorts of DDoS attacks, regardless of whether it is UDP surge, TCP SYN surge, Ping of Death or Smurf attack in light of conduct of the attack.

B. Defense The second part is defense, where it is utilized to piece UDP surge, TCP SYN surge, Ping of Death and Smurf attack before it ranges to the system as appeared in Fig. 9.

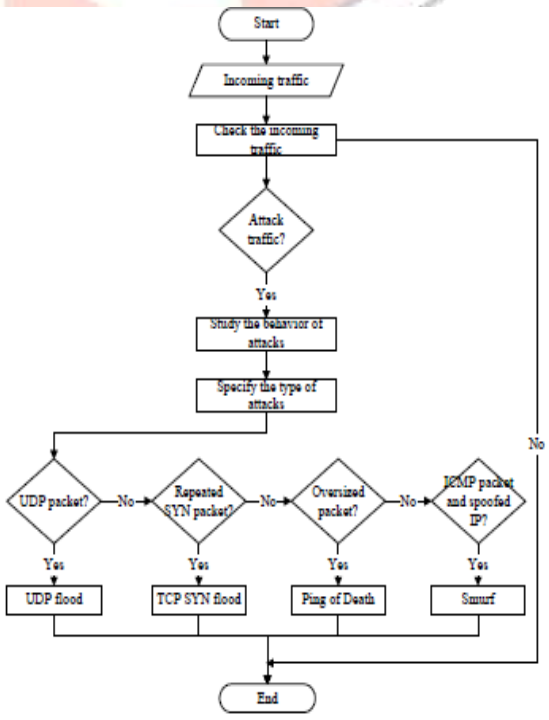

Fig. 8. Process of detection.

If the number of packets received is larger than 100 packets/second, the packet will be dropped

consequently by the proposed defense algorithm. The half and half of Snort and IPTables are utilized as full profound packet investigation, diminish the speed of approaching packets and control the utilization of system transmission capacity.

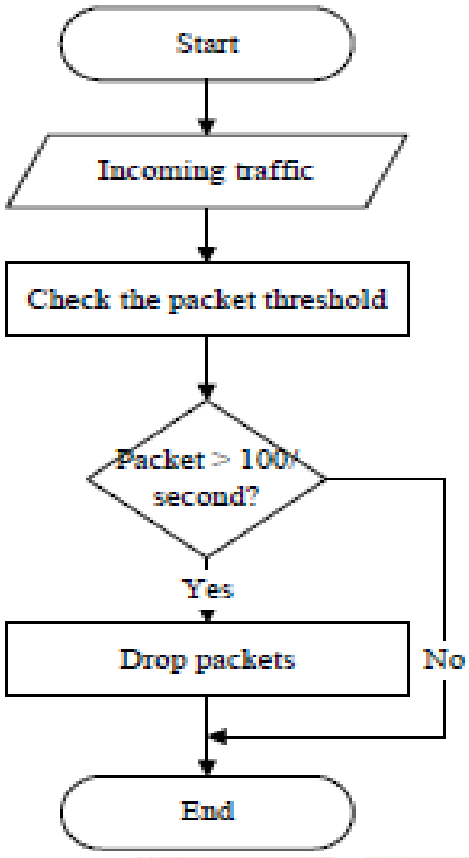

Fig. 9. Process of defense.

The proposed barrier algorithm will guarantee just clean movement can enter into the system. The greatest quality of this barrier algorithm is that secures the system regardless of whether a DDoS attack has been distinguished.

C. Report of Attacks: The report of attacks is extremely basic where it is utilized to log the sorts of DDoS attacks distinguished as appeared in Fig. 10. The quality of the report of attacks is delivered persistently progressively perceivability into undesirable movement and it will have the accompanying points of interest of the attack:

1) Types of DDoS attacks – There are four kinds of DDoS attacks: UDP surge, TCP SYN surge, and Ping of Death and Smurf attack.

2) Packet measure – Specifies the packet estimate, either irregular estimated or larger than usual of packet.

3) Severity level – Risk of attack, possibly it is low, medium or abnormal state.

4) Detection time – Duration of the attacks surge the system.

5) Attacker source – The address that the packet was sent from the aggressor, it is possible that it is utilizing a genuine IP address or mock IP address.

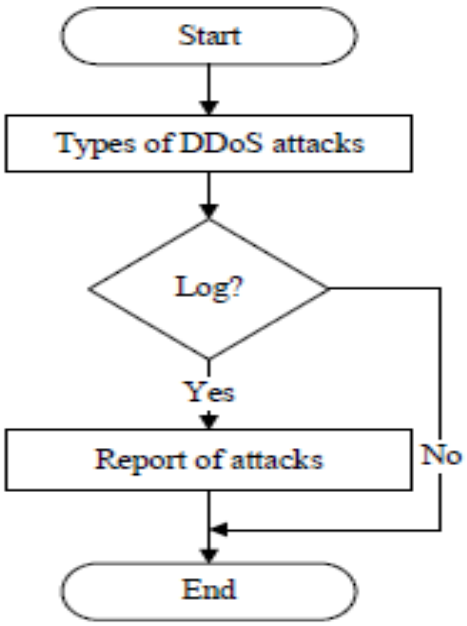

Fig. 10. Process of report of attacks.

5. Experimental Design

The experimental design of the proposed algorithm to be tested practically as shown in Fig. 11.

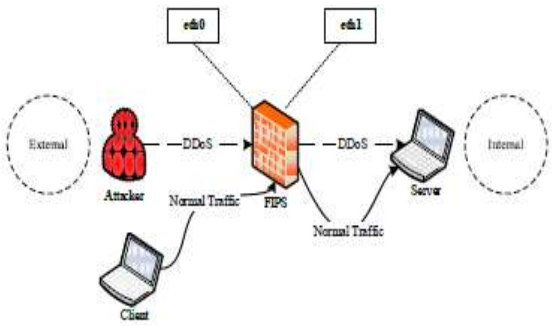

Fig. 11. Experimental setup.

In this test setup, four kinds of DDoS attacks: UDP surge, TCP SYN surge, Ping of Death and Smurf attack should be created by applying Putty Terminal for Windows and Terminal-based Wireshark (TShark). Firewall and hybrid of Snort and IPTables (FIPS) are required with a specific end goal to actualize and test the proposed algorithms infused into FIPS when in doubt based discovery towards approaching packets. The proposed algorithms will indicate the kinds of DDoS attacks, regardless of whether it is UDP surge, TCP SYN surge, Ping of Death or Smurf attack in light of the conduct of attacks. At that point, the half and half of Snort and IPTables will capacity to drop the packet consequently before the attack spans to the system framework. The proposed algorithms will be estimated as far as false positive rates and location precision. As indicated by, false positive rates is an ordinary or clean activity erroneously distinguished as an attack, while the discovery precision is a capacity of identifier to recognize an attack with higher exactness esteem for improving identification comes about.

6. Conclusion

This paper audited four kinds of DDoS attacks and their belongings and furthermore a few current DDoS recognition and resistance algorithm. The proposed identification and defense algorithm will be assessed utilizing the current Intrusion Detection and Prevention instrument to decide if it is the best algorithm to relieve the DDoS attacks towards a system situation. This exploration will then continue with the execution of the proposed algorithm to gauge false positive rates and identification exactness.

7. References

[1] M. Buvaneswari and T. Subha, "IHONEYCOL: A distributed collaborative approach for mitigation of DDoS attack," *International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 340-345.

[2] H. Guerid, A. Serhrouchni, M. Achemlal and K. Mittig, "A novel traceback approach for direct and reflected ICMP attacks," *IEEE Conference on Network and Information Systems Security (SAR-SSI)*, pp. 1-5, 2011.

[3] N. B. I. Al-Dabagh and I. A. Ali, "Design and implementation of artificial immune system for detecting flooding attacks," *International Conference on High Performance Computing and Simulation (HCOMPUTERS)*, pp. 381-390, 2011.

[4] M. Vijayalakshmi, D. S. M. Shalinie and A. A. Pragash, "IP traceback system for network and application layer attacks," *IEEE International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 439-444, 2012.

[5] Shaik Kareem and Maddali M.V.M. Kumar, "A New Second - Order Joint Congestion Control and Routing Framework Based On a Primal - Dual Interior - Point Approach," International Journal of Scientific Engineering and Technology Research, pp. 1948-1954, 2017.

[6] S. Saurabh and A. S. Sairam, "Linear and remainder packet marking for fast IP traceback," *IEEE Fourth International Conference on Communication Systems and Networks (COMSNETS 2012),* pp. 1-8, 2012.

[7] C. James and H. A. Murthy, "Decoupling non-stationary and stationary components in long range network time series in the context of anomaly detection," *IEEE 37th Conference on Local Computer Networks (LCN),,* pp. 76-84, 2012.

[8] S.-H. Lim and J.-H. Kim, "Dynamic security level changing strategy using attack predictions-Case study of TCP SYN attacks," *IEEE International Conference on IT Convergence and Security (ICITCS),* pp. 1-4, 2014.

[9] P. M. Priya, V. Akilandeswari, S. M. Shalinie, V. Lavanya, and M. S. Priya, "The Protocol Independent Detection and Classification (PIDC) system for DRDoS attack," *International Conference on Recent Trends in Information Technology*, pp. 1-7, 2014.

[10] McAfee Labs, "McAfee labs threats report," *McAfee*, Santa Clara, 2015.

[11] T. Reagor. 12 types of DDoS attacks used by hackers. [Online]. Available: http://www.rivalhost.com

[12] Imperva, "The top 10 DDoS attack trends," *Imperva*, California, 2015.

[13] Neustar, "The danger deepens: Neustar's annual DDoS attacks and impact report," pp. 1-14, 2014.

[14] S. Sivabalan and Radcliffe, "A novel framework to detect and block DDoS attack at the application layer," in *Porc. IEEE TENCON Spring Conference*, 2013, pp. 578-582.

[15] B. Rawal, H. Ramcharan, and A. Tsetse, "Emergence of DDoS resistant augmented split architecture," *IEEE High Capacity Optical Networks and Emerging/Enabling Technologies*, pp. 37-43, 2013.

[16] S. S. Kolahi, K. Treseangrat and B. Sarrafpour, "Analysis of UDP DDoS flood cyber attack and defense mechanisms on web server with Linux Ubuntu 13," in *Porc. International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2015, pp. 1-5.

[17] K. Geetha and N. Sreenath, "SYN flooding attack Identification and analysis," *International Conference on Information Communication & Embedded Systems*, pp. 1-7, 2014.

About Authors:

U. Leela Krishna is currently pursuing his MCA in MCA Department, St. Ann's College Engineering and Technology, Chirala A.P. He received his Bachelor of Science from ANU.

Mr. Maddali M. V. M. Kumar received his Master of Technology in Computer Science & Engineering from JNTUK and currently pursuing his Ph.D. in Computer Science & Engineering from ANU. He is working as an Assistant Professor in the Department of MCA, St. Ann's College of Engineering & Technology. He is a Life Member in CSI, IAENG & ISTE. His research focuses on the Computer Networks, Mobile & Cloud Computing.